



UNITED STATES DEPARTMENT OF COMMERCE

U.S. Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

07/105998

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
---------------------------------	-------------	---	---------------------

EXAMINER
----------

ART UNIT	PAPER
----------	-------

20050809

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Please see attached Examiner's Amendment and interview summary.

<b>Interview Summary</b>	Application No.	Applicant(s)	
	09/705,998	JUTLA, CHARANJIT SINGH	
	Examiner	Art Unit	
	Jacob F. Betit	2164	

All participants (applicant, applicant's representative, PTO personnel):

(1) Jacob F. Betit. (3) \_\_\_\_\_

(2) Dr. Louis Hertzberg. (4) \_\_\_\_\_

Date of Interview: 09 August 2005.

Type: a) ☒ Telephonic b) ☐ Video Conference  
c) ☐ Personal [copy given to: 1) ☐ applicant 2) ☐ applicant's representative]

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☒ No.  
If Yes, brief description: \_\_\_\_\_

Claim(s) discussed: None.

Identification of prior art discussed: None.

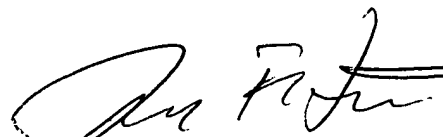
Agreement with respect to the claims f) ☐ was reached. g) ☐ was not reached. h) ☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The examiner requested permission to amend parts of pages 21 and 22 to fix errors with the reference numbers. Permission was granted.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

  
Examiner's signature, if required

### EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dr. Louis Hertzberg on 09-August-2005 (see attached interview summary).

The application has been amended as follows:

2. Replace the 3<sup>rd</sup> paragraph on page 21 with the following:

We first prove the theorems for the variants which employ sequences which are pair-wise independent. These are described in Fig-~~10~~ 11 and Fig-~~11~~ 12. They are different from the example embodiments (i.e. Figure 4 and Figure-~~9~~ 8) in that to generate a pair-wise independent sequence at least two new pseudo random numbers need to be generated (i.e. W1, #F: in Figure 11), as opposed to just one pseudo random number R in the example embodiments in Fig 4 and Fig-~~9~~ 8. The proof of security of the scheme in Fig-~~10~~ 11 (i.e. the one using pair-wise independent sequence) can then be generalized to prove the security of the example embodiment (i.e. the one using pair-wise additively-uniform sequence).

Art Unit: 2164

3. Replace the 1<sup>st</sup> line of the 4<sup>th</sup> paragraph on page 21 with the following:

In Fig-~~10~~ 11 (and also in Fig-~~11~~ 12) a subset construction is employed to produce the

4. Replace the 2<sup>nd</sup> paragraph on page 22 with the following:

The scheme in Fig-~~10~~ 11 will be referred to as the IACBC scheme. The scheme in Fig ~~11~~ 12 will be referred to as the IAPM scheme.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-4075. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

jfb  
9 Aug 2005

  
CHARLES RONES  
PRIMARY EXAMINER